



Vereinbarung über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung

Diese Vereinbarung über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung ist Teil der Nutzungsbedingungen von Joineer und bildet ein integrierender Bestandteil des Vertrages zwischen der Joineer AG (im Folgenden: Auftragnehmer) und dem Kunden (im Folgenden: Auftraggeber).

1 Einleitung, Geltungsbereich, Definitionen

- (1) Diese Vereinbarung regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.
- (3) In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Grundsätzlich sind Erklärungen schriftlich zu machen. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

Durchführung von Teambarometer-Intervallen auf Weisung des Auftraggebers. Hierfür werden Daten der Mitarbeitenden durch den Auftraggeber zur Verfügung gestellt.

Die Verarbeitung beruht auf der zwischen den Parteien geschlossenen Vertrag (im Folgenden „Hauptvertrag“).

Teambarometer bezieht sich auf das von Joineer entwickelte webbasierte Befragungstool, das mithilfe der Erhebung von qualitativen und quantitativen Daten die Mitarbeiterzufriedenheit und andere Rückschlüsse erkennen lässt.

2.2 Dauer

Die Verarbeitung beginnt mit Abschluss des Hauptvertrages und erfolgt auf unbestimmte Zeit bis zur Kündigung des Hauptvertrags durch eine Partei.

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art der Verarbeitung

Die Verarbeitung ist folgender Art: Erfassen, Speicherung, Aufbereitung, Auswertung, Verknüpfung und Löschung von Daten.

3.2 Zweck der Verarbeitung

Der zugrundeliegende Zweck der Verarbeitung ist in der Leistungsbeschreibung des Hauptvertrages geregelt.

3.3 Art der Daten

Es werden folgende Daten verarbeitet:

- Firmenname, Vorname, Nachname, E-Mailadresse, Zuordnung zur Organisationseinheit/Team. Auf Wunsch des Auftraggebers können auch die Mobilnummer sowie durch den Auftraggeber zu bestimmende soziodemographische Angaben verarbeitet werden.

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Beschäftigte des Auftraggebers

4 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemässer Datenverarbeitung.
- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut gemacht wurden. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
- (5) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten. Die erforderlichen Angaben und Dokumentationen sind zur Verfügung zu halten.
- (6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (7) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (8) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenkonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (9) Die Auftragsverarbeitung erfolgt grundsätzlich in der Schweiz oder der EU. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.

5 Sicherheit der Verarbeitung

- (1) Die im Anhang 1 beschriebenen Datensicherheitsmassnahmen gelten als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
- (2) Die Datensicherheitsmassnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (3) Soweit die getroffenen Sicherheitsmassnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten strikt nach Kunden-ID getrennt werden.
- (5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen sowie Backups, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist. Der Auftragnehmer behält sich vor, vollständig anonymisierte Daten des Auftraggebers zu Analyse-Zwecken im Rahmen der Optimierung der Dienstleistungen des Auftragnehmers zu verwenden.
- (6) Die Verarbeitung von Daten im Auftrag des Auftraggebers ausserhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist zulässig, soweit der Auftragnehmer sicherstellt, dass ein der Betriebsstätte gleichwertiges Schutzniveau besteht.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung des Hauptvertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
- (2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in dieser Vereinbarung vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

- (4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Massnahmen sorgfältig aus.
- (6) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
- (7) Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
- (5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie in dieser Vereinbarung vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstösse des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstösst. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (3) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

- (1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, werden diese durch den Auftragnehmer gelöscht. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Alte Backups (vergangene verschlüsselte Systemsicherungen) können aus technischen Gründen nicht vernichtet werden. Der Auftragnehmer verpflichtet sich jedoch ausdrücklich, keine wegen Beendigung des Auftrags gelöschten Daten wiederherzustellen.
- (2) Dokumentationen, die dem Nachweis der ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Hauptvertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

12 Vergütung

Die Vergütung des Auftragnehmers ist abschliessend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieser Vereinbarung erfolgt nicht.

13 Datenschutzrechtlicher EU-Vertreter

Wir verfügen über nachfolgende Datenschutz-Vertretung gemäss Art. 27 DSGVO im Europäischen Wirtschaftsraum (EWR) einschliesslich Europäischer Union (EU) und Fürstentum Liechtenstein als zusätzliche Anlaufstelle für Aufsichtsbehörden und betroffene Personen für Anfragen im Zusammenhang mit der Datenschutz-Grundverordnung (DSGVO):

VGS Datenschutzpartner GmbH
Am Kaiserkai 69
20457 Hamburg
Deutschland

info@datenschutzpartner.eu

<https://datenschutzpartner.eu/>

14 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Hauptvertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der jeweils anderen Partei auch über die Beendigung des Hauptvertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Massnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Die Grundlage dieses Vertrages wurde von activemind erstellt und von Joineer angepasst.

Anlage 1 – technische und organisatorische Massnahmen

1. Vertraulichkeit

a. Zutritts-/Zugangskontrolle

Die Daten werden in einem Rechenzentrum des Anbieters "Cloudscale" gespeichert. Dieser erfüllt alle gängigen Sicherheitsanforderungen und ist ISO zertifiziert.

Die Daten werden auf UNIX Servern und nicht auf PCs gespeichert. Diese sind mit persönlichen Zertifikaten gesichert.

b. Zugriffskontrolle

- i. Technische Massnahmen: Der Zugriff wird ausschliesslich über persönliche Verschlüsselungszertifikate gewährt
- ii. Organisatorische Massnahmen
 1. Differenzierung administrativer Aufgaben
 2. Einsatz eines Berechtigungskonzeptes
 3. Verwaltung Benutzerrechte durch Administratoren

c. Trennung

- i. Technische Massnahmen
 1. Physikalische Trennung (Systeme / Datenbanken / Datenträger)
 2. Trennung von Produktiv- und Testumgebung
- ii. Organisatorische Massnahmen
 1. Festlegung von Datenbankrechten
 2. Steuerung über Berechtigungskonzept

2. Integrität

a. Eingabekontrolle

- i. Technische Massnahmen
 1. Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ii. Organisatorische Massnahmen
 1. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
 2. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

b. Weitergabekontrolle

- i. Technische Massnahmen
 1. Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- ii. Organisatorische Massnahmen
 1. Weitergabe in anonymisierter oder pseudonymisierter Form

3. Verfügbarkeit und Belastbarkeit

Zur Sicherung der Daten werden tägliche Backups auf eigens dafür vorgesehenen Backup Servern durchgeführt.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

- a. Datenschutzmanagement
 - i. Alle Mitarbeitenden des Auftragnehmers sind auf Vertraulichkeit und die Wahrung des Datengeheimnisses verpflichtet.
- b. Incident-Response-Management
 - i. Technische Massnahmen
 - 1. Einsatz von Firewall und regelmässige Aktualisierung
 - ii. Organisatorische Massnahmen
 - 1. Dokumentation von Sicherheitsvorfällen und Datenpannen
- c. Datenschutzfreundliche Voreinstellungen
 - i. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich
- d. Auftragskontrolle (Outsourcing an Dritte)
 - i. Es findet kein Outsourcing an Dritte statt. Sollte ein Outsourcing an Dritte durch den Auftragnehmer vorgesehen werden, holt er vorgängig das schriftliche Einverständnis des Auftraggebers ein.

Anlage 2 – Unterauftragnehmer

Liste der aktuellen Unterauftragnehmer:

Name	Anschrift	Art der Leistung
Cloudscale.ch Ltd.	Doerflistrasse 50, 8050 Zürich	Server Hosting
Twilio	Rosenheimer Str. 143c, 81671 München	SMS Sending
Mailgun (Hosting aller Daten ausschliesslich in der EU unter voller Einhaltung des DSGVO)	112 E Pecan St. #1135 San Antonio, Texas	Email Sending
Piwikpro	Kurfürstendamm 21, D-10719 Berlin	Analytics
Intercom	18-21 St. Stephen's Green, Dublin	Support chat
New Relic	Klausstrasse 33, 8024 Zürich	Log Management & Observability

Anlage 3 – Datenschutzbeauftragter

Thomas Bürli

thomas.buerli@joineer.com

Tel: +41 44 510 38 00